Vurdering av kritikaliteten på leveransen til IKT-leverandøren (4.2.1)

| Kriterier | Vurdering i analysen | Evaluering (1–5) | Vekting |
|---|---|---|---|
| **Kritikalitet** | **Er denne tjenesten ansett som essensiel for noen forretningsprosesser som er klassifisert som kritiske ifølge forretnings konsekvensanalysen (BIA)?** | 1–5 | 40–60% |
| | Ikke-kritisk score: 1 | | |
| | Kritisk score: 5 | | |
| **Avhengighet** | **Hvor avhengig er virksomheten av IKT-tjenesten som leverandøren tilbyr for at den kritiske/viktige funksjonen skal være tilgjengelig?** | 1–5 | 40–60% |
| | Ingen avhengighet score: 1 | | |
| | Kritisk avhengighet score: 5 | | |
| **Merknad 1:** Vektene (kolonne E) er et forslag basert på tidligere erfaringer med evaluering av IKT-leverandører. Hver virksomhet kan bruke en annen vektfordeling. | | | |
| **Merknad 2:** I vurderingen er påvirkning på tjenesten hovedsakelig vurdert, mens sannsynlighet bevisst er utelatt. | | | |
| | | | |
| **Skåringskriterier for kritikalitet (baseres på virksomhetens BIA)** | **Skåringskriterier for avhengighet** | | |
| 1. Kritikalitet er ingen eller ubetydelig. | 1. Ingen avhengighet: Det er ingen avhengighet av denne IKT-leveransen | | |
| 2. Kritikalitet er lav. | 2. Lav avhengighet: IKT-leveransen har liten innvirkning og kan enkelt erstattes eller kompenseres for. | | |
| 3. Kritikalitet er moderat. | 3. Moderat avhengighet: IKT-leveransen har en betydelig, men håndterbar innvirkning på systemet eller prosessen. | | |
| 4. Kritikalitet er stor/viktig | 4. Høy avhengighet: IKT-leveransen er svært viktig og vanskelig å erstatte, noe som kan skape utfordringer ved fravær eller feil. | | |
| 5. Kritikalitet er ekstrem/kritisk | 5. Kritisk avhengighet: IKT-leveransen er avgjørende for systemets funksjon, og dens fravær eller svikt vil føre til store konsekvenser. | | |

| | | |
|---|---|---|
| **Ikke-kritisk/viktig IKT-leverandør** | Total score mellom 1 og 3 | Årlig oppfølging av IKT-leverandør og avtaler. |
| **IKT-leverandører av betydning** | Total score mellom 3 og 4 | Kvartalsvis oppfølging av IKT-leverandør og avtaler. Vurder behov for etablering av exitplan. Vurder gjennomgang av tredjepartsattestasjoner. |
| **Kritisk/viktige IKT-leverandører** | Total score mellom 4 og 5 | Jevnlig oppfølging av leverandører og avtaler, samt årlig gjennomgang av tredjepartsattestasjoner. Tiltak som implementeres for leverandøren bør være risikoreduserende tiltak, identifisering av alternative leverandører, tettere samarbeid, utarbeidelse av exitplan. |

Standard sjekkliste for risikovurdering av IKT-leverandører (4.2.2)

| # | Kontrollpunkt | Beskrivelse | Status | Kommentar |
|---|---|---|---|---|
| 1 | **Finansielle vurderinger** | Gjennomgå IKT-leverandørens økonomiske rapporter for å vurdere deres stabilitet og levedyktighet | | |
| 2 | **Informasjonssikkerhet** | Kartlegg sikkerhetstiltakene IKT-leverandøren har implementert for å beskytte data og systemer | | |
| 3 | **Tidligere erfaring** | Innhent referanser fra andre kunder for å vurdere IKT-leverandørens pålitelighet og kvalitetsnivå | | |
| 4 | **Enkelhet å bytte** | Hvor enkelt er det å bytte fra en bestemt IKT-leverandør til en annen for dette produktet eller tjenesten? | | |
| 5 | **Underleverandører** | Identifiser om IKT-leverandøren bruker underleverandører, og vurder deres potensielle risiko | | |
| 6 | **Konsentrasjonsrisiko** | Kartlegg antall tjenester eller produkter som allerede er kjøpt fra samme IKT-leverandør, og vurder om leverandørkonsentrasjonen er akseptabel eller om det er behov for diversifisering | | |
| 7 | **Kritisk IKT-leverandør i EU** | Sjekk om IKT-leverandøren er klassifisert som kritisk i henhold til leverandørregisteret som skal opprettes under DORA iht. Register of Information. Vurder hvilke konsekvenser denne klassifiseringen kan ha for din virksomhet. | | |

Standardiserte maler for kontrakter og vedlegg (4.3.1)

| # | Kontrollpunkt | Beskrivelse | Status | Kommentar |
|---|---|---|---|---|
| 1 | **Sikkerhetskrav** | Inkluder spesifikke krav til datasikkerhet, personvern, tilgangskontroll og hendelseshåndtering i kontrakten, i tråd med DORA. | | |
| 2 | **Bruk av underleverandører** | Still krav til at IKT-leverandør skal opplyse om hvilke underleverandører de benytter og hvilke tjenester de leverer som er relevant for egen leveranse. | | |
| 3 | **Endringshåndtering** | Definer prosedyrer for håndtering av endringer i tjenestene eller sikkerhetskravene, inkludert hvordan slike endringer skal kommuniseres og implementeres. Avtale må ha rom for vilkårsendringer som følge av endring i lovgivning eller rettspraksis, og virksomheten må faktisk følge opp dette dersom nødvendig. | | |
| 4 | **Rapportering og revisjon** | Etabler krav til regelmessig rapportering og revisjon for å overvåke IKT-leverandørens etterlevelse av attestasjonstandarder og operasjonell motstandskraft, eks. ISAE 3000 med relevant innretning, SOC-rapporter eller tilsvarende standard. | | |
| 5 | **Kontinuitetsplanlegging** | Inkluder krav om beredskapsplaner og kontinuitetsplaner for å sikre at tjenestene kan opprettholdes under ulike krisesituasjoner. | | |
| 6 | **Sanksjoner og konsekvenser** | Beskriv sanksjoner eller konsekvenser ved manglende etterlevelse av avtalte krav, for å sikre at IKT-leverandøren tar sine forpliktelser på alvor. | | |

| | | | | |
|---|---|---|---|---|
| **7** | **Exitplaner** | Det må etableres kriterier for å gå ut av kontrakten/avbryte samarbeidet med IKT-leverandøren. Avtale hvordan avtalen kan avsluttes, inkludert krav til tilbakeføring av data og oppsigelsestid. | | |
| **8** | **Tydelige ansvarsområder** | Definer hvilken part som har ansvar for ulike deler av tjenesten, inkludert oppfølging av sikkerhet og drift. | | |

Standard sjekkliste for IKT-leverandøravtaler (4.3.2)

| # | Kontrollpunkt | Krav i | Status | Kommentar |
|---|---|---|---|---|
| 1 | Rettigheter og forpliktelser mellom partene skal være tydelig definert, skriftlig og tilgjengelig for alle parter. Det skal inneholde nivået | 30.1 | | |
| 2 | Er leverandør å regne som en kritisk eller viktig leverandør? (Ja/Nei) | - | | |
| **Krav til avtaler med alle IKT-leverandører** | | | | |
| 3 | Inneholder avtalen informasjon om hva som skal leveres? | 30.2.a | | |
| 4 | Benytter IKT-leverandøren underleverandører? | 30.2.a | | |
| 5 | Inneholder avtalen en beskrivelse av vilkårene for underleverandøren? | 30.2.a | | |
| 6 | Beskriver avtalen lokasjonen hvor tjenesten leveres fra? | 30.2.b | | |
| 7 | Inkluderer avtalen beskrivelse av hvor data, inkludert personopplysninger, skal lagres og behandles? | 30.2.b | | |
| 8 | Inkluderer avtalen beskrivelse av varsling i forkant av planlagte endringer i slike lokasjoner? | 30.2.b | | |
| 9 | Inneholder avtalen beskrivelse av hvordan data, inkludert personopplysninger, sikres iht. konfidensialitet, integritet og tilgjengelighet | 30.2.c | | |
| 10 | Inneholder avtalen bestemmelser om sikring av adgang, gjenoppretting og tilbakelevering av data, inklusivt personopplysninger i et tilgjengelig format ved avvikling, avbrudd, oppsigelse eller konkurs | 30.2.d | | |
| 11 | Beskriver avtalen ulike servicenivåer, revisjoner og oppdatering av disse? | 30.2.e | | |

| | | | | |
|---|---|---|---|---|
| **12** | Inkluderer avtalen forpliktelser til bistand fra IKT-leverandøren ved IKT-hendelser til avtalt pris, i den grad pris ikke er avtalt er det uten ekstra kostnad? | 30.2.f | | |
| **13** | Forplikter IKT-leverandøren seg til å samarbeide fullt ut med kompetente myndigheter eller de selskap/personer virksomheten utnevner? | 30.2.g | | |
| **14** | Beskriver avtalen oppsigelsesrett og minimums varslingsperiode for terminering av avtalen, som tillater operativ drift iht. myndighetenes krav? | 30.2.h | | |
| **15** | Beskrives IKT-leverandørens vilkår for deltakelse i finansforetakets program- og opplæring for digital motstandsdyktighet? | 13.6<br>30.2 (i) | | |
| **Krav til avtaler med IKT-leverandører klassifisert som kritiske eller viktige (30.3)**<br>*Følgende krav skal kontraktsfestes i avtalen* | | | | |
| **16** | Beskriver avtalen en fullstendig SLA, inkludert oppdateringer og revisjoner, med presise kvalitative og kvantitative ytelsesmål innenfor avtalte tjenestenivå? | 30.3.a | | |
| **17** | Beskriver avtalen hvordan krav i SLA-en overvåkes, samt hvordan korrigerende tiltak kan iverksettes uten unødig forsinkelse når avtalte SLA-nivå ikke oppfylles? | 30.3.a | | |
| **18** | Beskrives oppsigelsesfrister og rapporteringsfrister fra leverandøren, samt varsling om enhver utvikling som kan ha vesentlig innvirkning på evnen til å effektivt levere IKT-tjenester som støtter kritiske eller viktige funksjoner i tråd med avtalte SLA-krav? | 30.3.b | | |

| | | | | |
|---|---|---|---|---|
| **19** | Beskriver avtalen krav om implementering og testing av forretningskontinuitetsplaner, etablering av IKT-sikkerhetstiltak, verktøy og retningslinjer som sikrer et godt nok sikkerhetsnivå for levering av tjenester, i samsvar med gjeldende regulatoriske rammeverk? | 30.3.c | | |
| **20** | Beskriver avtalen hvordan IKT-leverandøren skal delta og fullt ut samarbeide med virksomhetens TLPT. | 26<br>27<br>30.3.d | | |
| **21** | Beskriver avtalen krav til ubegrenset rettighet til tilgang, inspeksjon og revisjon fra virksomheten, tilsynsmyndighet eller oppnevnt tredjepart? Inkl. rett til å ta kopier av relevant dokumentasjon på stedet hvis kritisk for driften. | 30.3.e (i) | | |
| **22** | Beskriver avtalen leverandørens plikt til å samarbeide fullt ut under inspeksjon og revisjoner på stedet? | 30.3.e (iii) | | |
| **23** | Inkluderer avtalen leverandørens plikt til å gi detaljer om omfang, prosedyrer som skal følges og hyppigheten av slike inspeksjoner og revisjoner? | 30.3.e (iv) | | |
| **24** | Inkluderer avtalen en beskrivelse av exit-strategi, med særlig fokus på obligatorisk tilstrekkelig overgangsperiode som både kan sikre fortsettelse av leveranse, alternativt mulighet til migrering av løsning til annen IKT-leverandør, eventuelt til interne løsninger hos virksomheten? | 30.3.f | | |

Sjekkliste oppfølgning av IKT-leverandører (4.4.1)

| # | Kontrollpunkt | Beskrivelse | Status | Kommentar |
|---|---|---|---|---|
| 1 | **Styring og kontroll** | Sikre at det er etablert tilfredsstillende styring og kontroll. | | |
| 2 | **Risikostyring** | Sikre at det er tilfredsstillende risikostyring. | | |
| 3 | **Hendelse/respons** | Sikre at det er etablert et hensiktsmessig regime for å respondere på ulike typer hendelser hos oppdragstaker og dens underleverandører, slik at oppdragsgiver kan rapportere eventuelle rapporteringspliktige hendelser til Finanstilsynet iht. DORA 19 (1) samt dekke forpliktelser i DORA 17 (2). | | |
| 4 | **Kontunitetstesting** | Sikre at foretakets krav til gjenoppretting (RTO/RPO/ MTPD) er ivaretatt og dokumentert i rapporter fra utført beredskaps- og kontinuitetstesting for de kritiske og viktige prosessene. | | |
| 5 | **Sikkerhetstesting** | Sikre at det gjennomføres tilstrekkelige sårbarhets- og penetrasjonstester og andre typer sikkerhetstesting. | | |
| 6 | **IKT-sikkerhetspolicy** | Sikre at kravene i foretakets IKT-sikkerhetspolicy er ivaretatt. | | |
| 7 | **Endrings-håndtering** | Sikre at kvaliteten på endringshåndteringen er ivaretatt. Foretaket bør blant annet ha oversikt over antall feil som følge av endringer. | | |
| 8 | **Risiko- og trusselovervåking** | Sikre at det er etablert betryggende risiko- og trusselovervåking. | | |
| 9 | **Tilgangsstyring** | Sikre at system og rutiner for identitets- og tilgangsstyring (IAM) er etablert. | | |
| 10 | **Logging** | Sikre at den etablerte system- og applikasjonsloggingen har tilstrekkelig omfang og kvalitet. | | |

| | | | | |
|---|---|---|---|---|
| **11** | **Eskalering** | Sikre at det er etablert klare rapporteringslinjer og eskaleringsstrukturer for å sikre at regulatoriske krav er ivaretatt. | | |
| **12** | **Attestasjoner** | Få tilsendt ISAE 3000 / 3402 / SOC1 / SOC2 eller tilsvarende standard. Må ha en plan for å følge opp rapporten internt, det er ikke nok å gi den videre til revisor. | | |

* Kravstillelse til IKT-leverandør vil avhenge av deres kritikalitet og/eller viktighet overfor selskapets øvrige forretningsprosesser. Kravstillelse av RTO/RPO/MTPD må settes iht. input fra BIA og vil kunne variere fra leverandør til leverandør.

Sjekkliste exitplan (4.5.1)

Denne sjekklisten er utarbeidet som et supplement til bruk under utarbeidelse av egne exitplaner. Listen er ikke uttømmende og gir ikke svar på hva som skal gjøres hvis svaret på et spørsmål er nei. Formålet med sjekklisten er for å sikre at de viktigste momentene i DORA er vurdert. Hvis svaret på noen av spørsmålene er nei, bør dette enten gjennomgås som et separat punkt eller kommenteres på hvorfor det ikke har blitt vurdert som et tillegg til planene.

| # | Tematikk | Kontrollspørsmål | Status | Kommentar |
|---|---|---|---|---|
| **Alternative Løsninger** | | | | |
| **1** | **Identifiser alternative leverandører** | Er det identifisert alternative IKT-leverandører? | | |
| **2** | **Internoverføring** | Er det mulighet for å flytte tjenesten in-house? | | |
| | | Er det gjort vurdering av modenhet for å kunne flytte tjenesten internt? | | |
| **3** | **Avvikling av tjeneste** | Må tjenesten avvikles grunnet manglende alternative løsninger? | | |
| | | Har man adressert risikoen på andre måter? | | |
| **Leverandørovergang** | | | | |
| **4** | **Tjenestefortsettelse under exit** | Er det etablert en plan for å sikre at tjenesten opprettholdes under overgangen/migrering? DORA 30.3 (f) | | |
| **5** | **Kunnskapsoverføring / kompetanseoverføring** | Er det etablert en plan / avtaler for kunnskapsoverføring fra IKT-leverandør? | | |
| **6** | **Tredjeparts kontrakter** | Er det vurdert om kontrakter med tredjeparter (underleverandører til IKT-leverandøren) skal være del av en exit plan? | | |
| **Risikohåndtering** | | | | |
| **7** | **Migrering** | Er det adressert risikoer knyttet til terminering / migrering? | | |
| | | Hvordan er identifiserte høy risiko aktiviteter eller andre risiko-momenter adressert? | | |
| **8** | **Kundepåvirkning** | Er det adressert risikoer knyttet til kundepåvirkning? | | |
| | | Er kunderelatert påvirkning adressert og planlagt for? | | |

| | | | | |
|---|---|---|---|---|
| **9** | **Regulatorisk** | Er det adressert risiko for å ikke kunne oppfylle regulatoriske krav? | | |
| | | Hvordan skal regulatoriske forpliktelser sikres i perioden. Herunder til AML og andre dokumentasjonskrav. | | |
| **10** | **Kontroller** | Hvilke ekstra kontroller og prosesser er det nødvendig å implementere i perioden? | | |
| **11** | **Roller** | Er det etablert tydelige roller og ansvar i eget selskap ved iverksettelse av Exit plan? | | |
| **12** | **Kompetanse** | Hvordan er kompetansen internt for å ta over, eller flytte til annen IKT-leverandør? | | |
| **Sikring av kundepåvirkning** | | | | |
| **13** | **Forstyrrelsesfri exit** | Er det sikret at en exit ikke nevneverdig påvirker kunde opplevelsen? | | |
| **14** | **Tjenestekvalitet** | Er det planlagt for påvirkning på og minimering av reduksjon av kontinuitet av tjenesten og kvalitet til kunder? | | |
| **15** | **Kommunikasjonsplan** | Er det utarbeidet en kommunikasjonsplan til kunder som kan bli påvirket av migrering eller exit fra IKT-leverandøren? | | |
| **Data- og Tilgangshåndtering** | | | | |
| **16** | **Datahåndtering** | Er det planlagt for utlevering, destruksjon eller overføring av data? | | |
| | | Har det blitt utarbeidet hvilken data som det er behov for? (Feil logger, kundedata, tilgangslogger, dokumentasjon m.m.) | | |
| **17** | **Fjerning av Tilgang** | Er det etablert en plan for fjerning av tilgang? | | |
| | | Hvordan skal dette gjennomføres? | | |
| | | Skal det etableres ekstra logging i perioden? | | |
| **18** | **Intellektuell eiendom (IP)** | Er det etablert en plan / avtale for hva som skjer med utviklet kode og annen IP? | | |
| **Økonomiske Vurderinger** | | | | |
| **19** | **Kostnadsvurdering** | Er kostnader relatert til alternativer under “alternative løsninger” vurdert? | | |
| **20** | **Migreringskostnader** | Er kostnader relatert til migrering evaluert? | | |

| | | | | |
|---|---|---|---|---|
| **21** | **Avslutningskostnad** | Har det blitt avtalt et vederlag for tidlig avslutning av avtale? Er det forskjeller avhengig av hvorfor den avsluttes tidlig? | | |
| **Testing og Gjennomgang av Plan** | | | | |
| **22** | **Testprosedyrer** | Er det etablert en plan for hvordan planen kan testes? (Desktop, table-top, annen måte) | | |
| | | Har man vurdert gjennomførbarhet av testingen? Kan man reelt få testet exit- planen, eller er det kun en compliance aktivitet? | | |
| | | Har man tilrettelagt for revisjonshistorikk og mulighet for endringer basert på test resultater? | | |
| **23** | **Leverandørinvolvering** | Har man vurdert til hvilken grad IKT-leverandøren må være involvert i testing av planen? | | |
| | | Har man vurdert hvilke deler av exitplanen som skal og kan deles med IKT-leverandør? | | |
| **Proporsjonalitet og Scenarier** | | | | |
| **24** | **Scenarier** | Er det etablert scenarier som vil trigge en exit? | | |
| | | Er scenarier, triggerpunkter og krav som kan utløse en exit forankret med IKT-leverandør? | | |
| **25** | **Påvirkning** | Er påvirkning på andre exit-planer og IKT-leverandører vurdert? | | |
| | | Er påvirkning på andre tjenester, som avhenger av denne tjenesten, vurdert? | | |
| **Intra-gruppe / allianse** | | | | |
| **26** | **Intra-gruppe / allianse** | Er det vurdert hvordan en exit fra avtalen/leverandørforholdet kan påvirke tjenestene innen intra-gruppen/alliansen? | | |
| | | Er det avklart hvordan en exit fra intra-gruppen/allianseavtalen vil påvirke de gjenværende tjenestene? | | |
| | | Hvordan vil en exit fra en IKT-leverandør i et intra-gruppeforhold/allianseforhold kunne påvirke andre avtaler som er inngått direkte med leverandøren? | | |